Computer Security: Principles and Practice

Fourth Edition

By: William Stallings and Lawrie Brown

Chapter 9

Firewalls and Intrusion Prevention Systems

The Need For Firewalls

- **Internet connectivity** is essential
  - However it creates a **threat**
- Effective means of **protecting LANs**
- Inserted between the premises network and the Internet to establish a **controlled link**
  - Can be a **single** computer system or a **set** of two or more systems working together
- Used as a **perimeter defense**
  - **Single choke point** to impose security and auditing
  - **Insulates** the internal systems from external networks

Firewall Characteristics

Design goals

All traffic from inside to outside, and vice versa, **must pass through** the firewall

Only authorized traffic as defined by the local security policy will be **allowed to pass**

The firewall itself is **immune to penetration**

Firewall Access Policy

- A critical component in the planning and implementation of a firewall is specifying a suitable **access policy**
  - This lists the **types of traffic authorized** to pass through the firewall
  - Includes **address ranges**, **protocols**, **applications** and **content types**
- This policy should be developed from the **organization's information security risk assessment and policy**
- Should be developed from a broad specification of **which traffic types the organization needs to support**
  - Then refined to detail the **filter elements** which can then be implemented within an appropriate **firewall topology**

Firewall Filter Characteristics

- **Characteristics** that a firewall access policy could use to filter traffic include:

IP address and protocol values

This type of filtering is used by **packet filter** and **stateful inspection firewalls**

Typically used to limit access to **specific services**

Application protocol

This type of filtering is used by an **application-level gateway** that relays and monitors the exchange of information for **specific application protocols**

User identity

Typically for **inside users** who identify themselves using some form of **secure authentication** technology

Network activity

Controls access based on considerations such as the time of request, rate of requests, or other **activity patterns**

Firewall Capabilities And Limits

Capabilities:

- Defines a single choke point
- Provides a location for monitoring security events
- Convenient platform for several Internet functions that are not security related
- Can serve as the platform for IPSec

Limitations:

- Cannot protect against attacks bypassing firewall
- May not protect fully against internal threats
- Improperly secured wireless LAN can be accessed from outside the organization
- Laptop, PDA, or portable storage device may be infected outside the corporate network then used internally

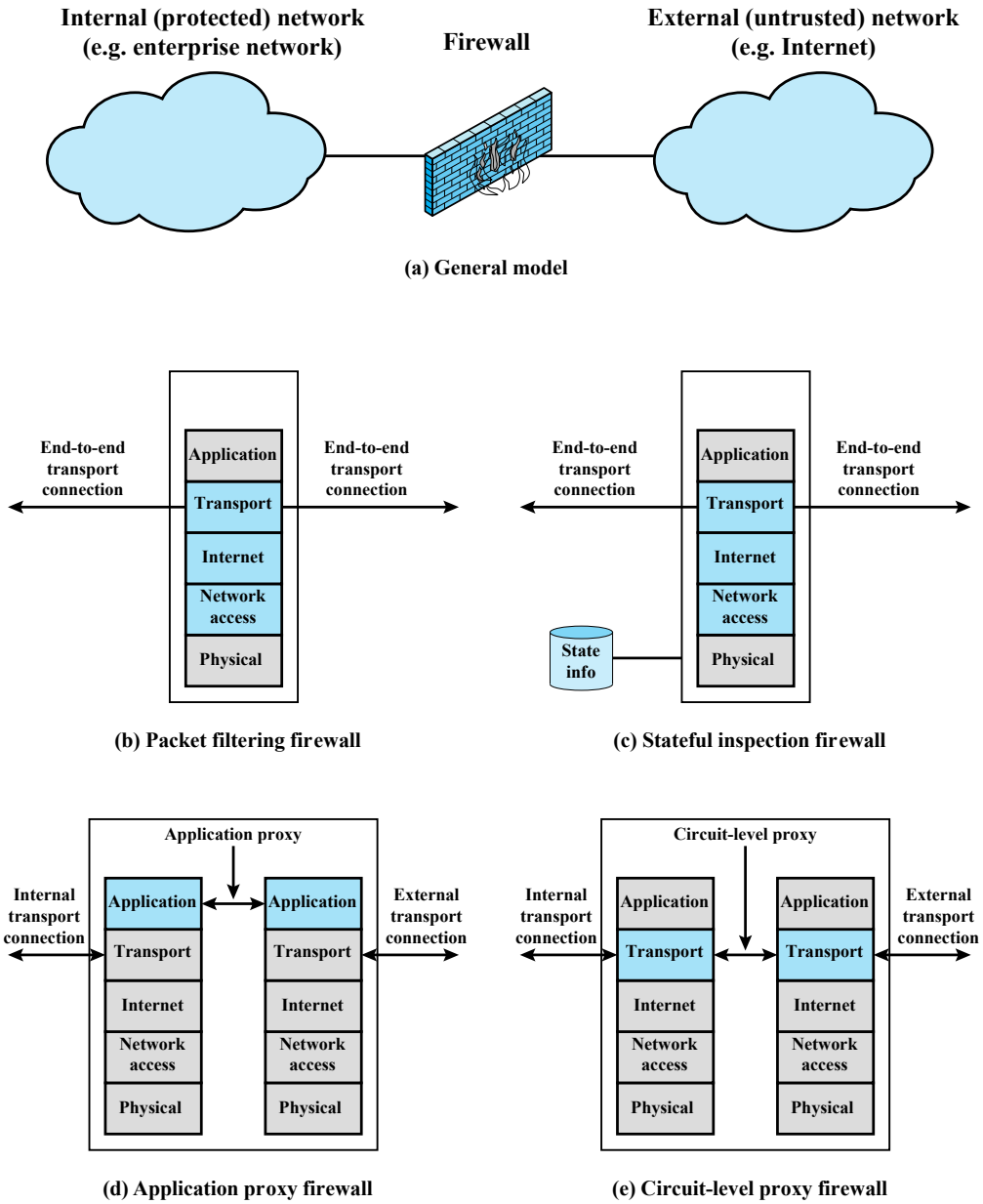


Figure 9.1 Types of Firewalls

Packet Filtering Firewall

- **Applies rules** to each incoming and outgoing IP packet
  - Typically a list of rules based on matches in the **IP** or **TCP header**
  - **Forwards** or **discards** the packet based on rules match

Filtering rules are based on information contained in a network packet
• Source IP address • Destination IP address • Source and destination transport-level address • IP protocol field • Interface

- Two default policies:
  - **Discard** - prohibit unless expressly permitted
    - More conservative, controlled, visible to users
  - **Forward** - permit unless expressly prohibited
    - Easier to manage and use but less secure

Table 9.1
Packet-Filtering Examples

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Packet Filter Advantages And Weaknesses

- Advantages
  - **Simplicity**
  - Typically **transparent to users** and are **very fast**
- Weaknesses
  - Cannot prevent attacks that employ **application specific vulnerabilities or functions**
  - Limited **logging functionality**
  - Do not support **advanced user authentication**
  - Vulnerable to attacks on **TCP/IP protocol bugs**
  - **Improper configuration** can lead to breaches

Stateful Inspection Firewall

Tightens rules for TCP traffic by creating a directory of outbound TCP connections

- There is an entry for each currently established connection
- Packet filter allows incoming traffic to high numbered ports only for those packets that fit the profile of one of the entries in this directory

Reviews packet information but also records information about TCP connections

- Keeps track of TCP sequence numbers to prevent attacks that depend on the sequence number
- Inspects data for protocols like FTP, IM and SIPS commands

Table 9.2
Example Stateful Firewall Connection State Table

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Application-Level Gateway

- Also called an **application proxy**
- Acts as a relay of **application-level traffic**
  - User contacts gateway using a **TCP/IP application**
  - User is **authenticated**
  - Gateway **contacts** application on remote host and **relays** TCP segments between server and user
- Must have **proxy code** for each application
  - May **restrict** application features supported
- Tend to be **more secure** than packet filters
- Disadvantage is the **additional processing overhead** on each connection

Circuit-Level Gateway

Circuit level proxy

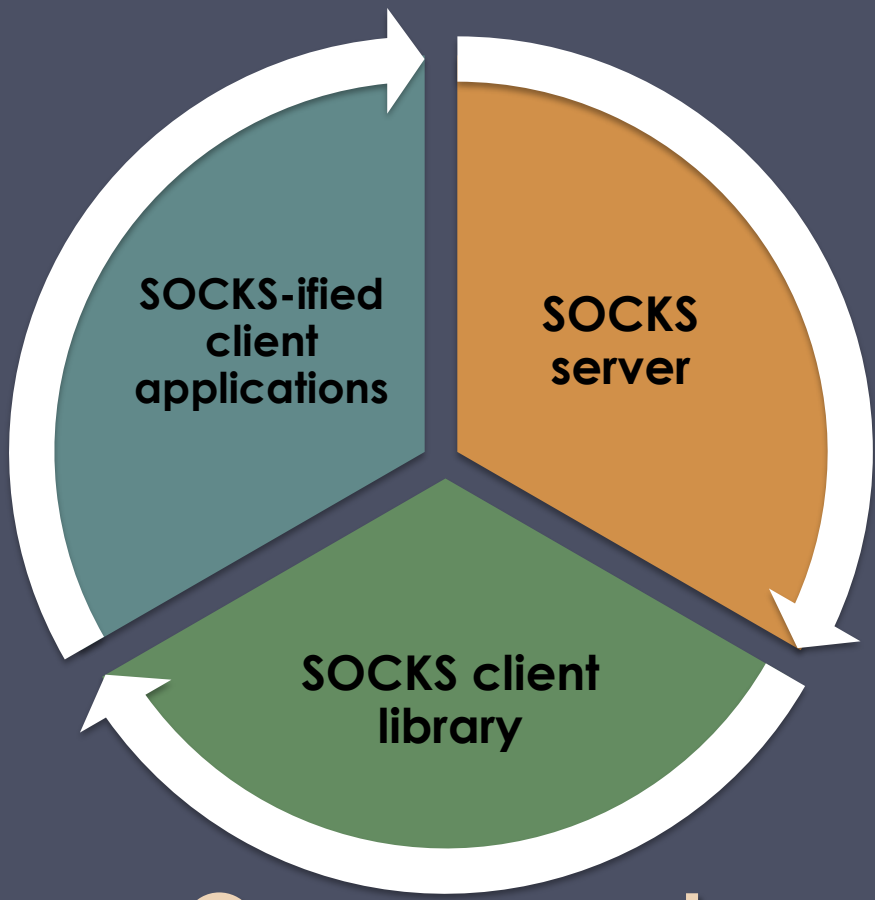
- Sets up **two TCP connections**, one between **itself** and a TCP user on an **inner host** and one on an **outside host**
- **Relays** TCP segments from one connection to the other **without examining contents**
- Security function consists of **determining which connections** will be allowed

Typically used when inside users are trusted

- May use **application-level gateway inbound** and **circuit-level gateway outbound**
- Lower overheads

SOCKS Circuit-Level Gateway

- **SOCKS v5** defined in RFC1928
- Designed to provide a framework for **client-server applications** in **TCP/UDP** domains to conveniently and securely use the **services of a network firewall**
- Client application contacts **SOCKS server**, authenticates, sends relay request
  - Server **evaluates** and either **establishes** or **denies** the connection



Components

Bastion Hosts

- System identified as a **critical strong point** in the network's security
- Serves as a **platform** for an **application-level** or **circuit-level gateway**
- Common characteristics:
  - Runs **secure O/S**, only **essential services**
  - May require **user authentication** to access proxy or host
  - Each proxy can **restrict features**, hosts accessed
  - Each proxy is **small**, **simple**, **checked** for security
  - Each proxy is **independent**, **non-privileged**
  - Limited disk use, hence **read-only code**

Host-Based Firewalls

- Used to **secure an individual host**
- Available in operating systems or can be provided as an **add-on package**
- **Filter and restrict packet flows**
- Common location is a **server**

Advantages:
• **Filtering rules** can be **tailored** to the host environment • Protection is provided **independent** of topology • Provides an **additional layer of protection**

Personal Firewall

- Controls traffic between a **personal computer** or workstation and the **Internet** or enterprise network
- For both **home** or **corporate** use
- Typically is a **software module** on a personal computer
- Can be housed in a **router** that connects all of the home computers to a DSL, cable modem, or other Internet interface
- Typically **much less complex** than server-based or stand-alone firewalls
- Primary role is to **deny unauthorized remote access**
- May also monitor **outgoing traffic** to detect and block worms and malware activity

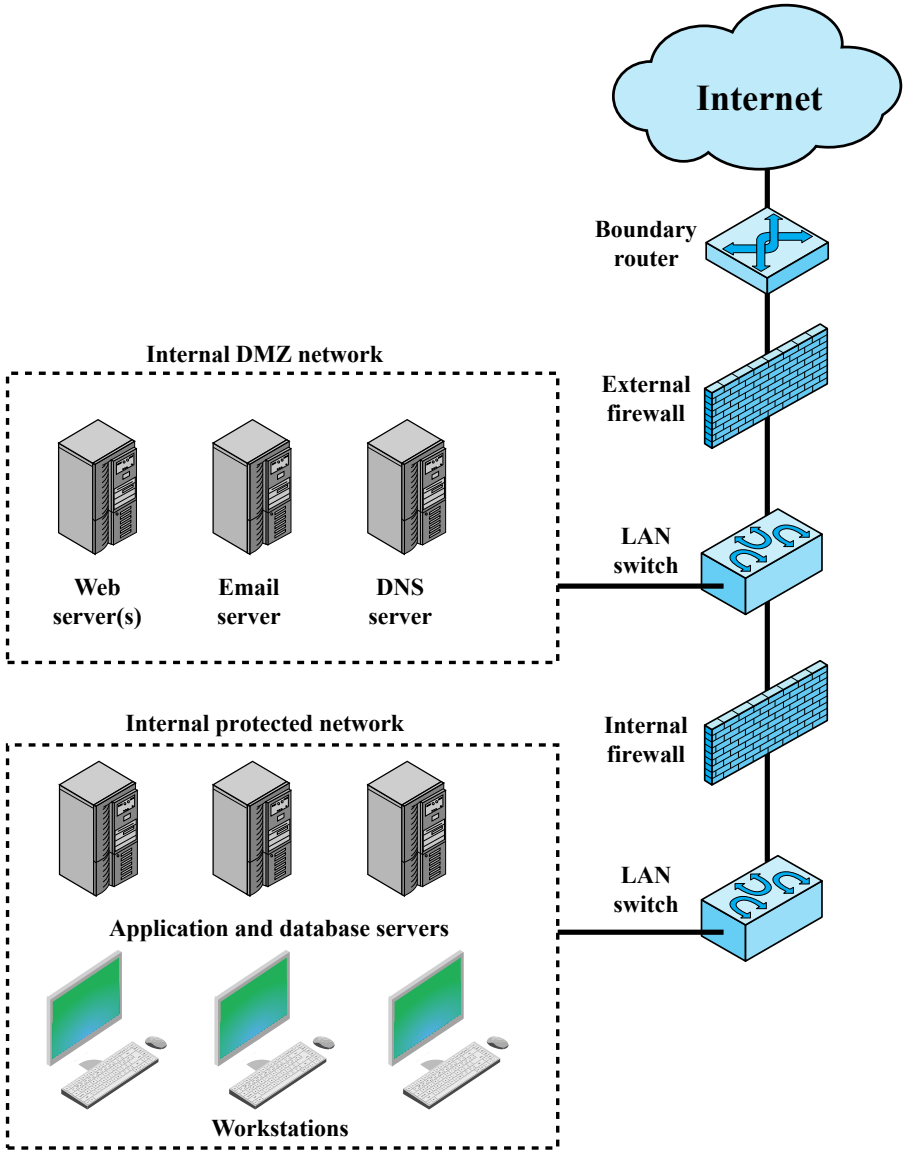


Figure 9.2 Example Firewall Configuration

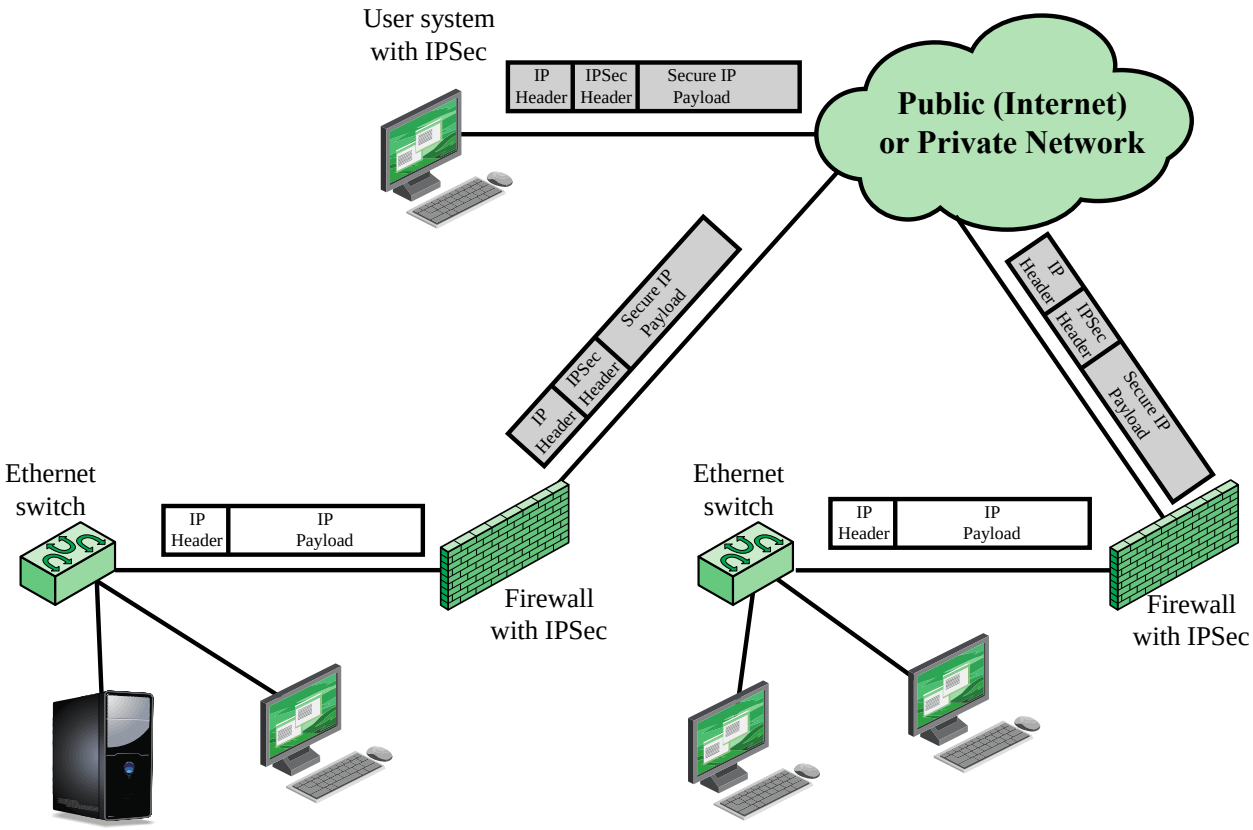


Figure 9.3 A VPN Security Scenario

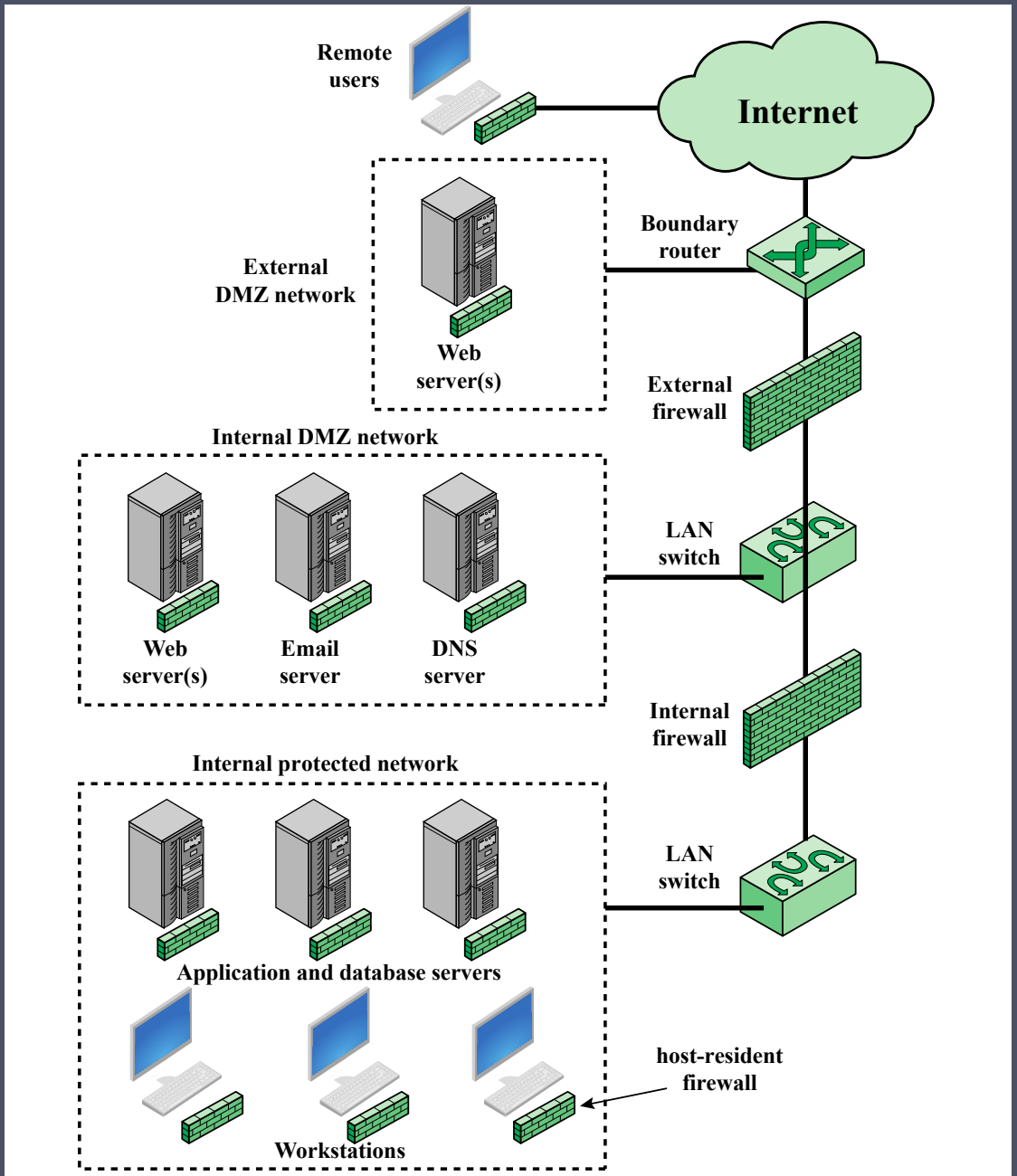


Figure 9.4 Example Distributed Firewall Configuration

Firewall Topologies

Host-resident firewall	• Includes personal firewall software and firewall software on servers
Screening router	• Single router between internal and external networks with stateless or full packet filtering
Single bastion inline	• Single firewall device between an internal and external router
Single bastion T	• Has a third network interface on bastion to a DMZ where externally visible servers are placed
Double bastion inline	• DMZ is sandwiched between bastion firewalls
Double bastion T	• DMZ is on a separate network interface on the bastion firewall
Distributed firewall configuration	• Used by large businesses and government organizations

Intrusion Prevention Systems (IPS)

- Also known as **Intrusion Detection and Prevention System** (IDPS)
- Is an **extension of an IDS** that includes the capability to attempt to **block** or **prevent** detected malicious activity
- Can be **host-based**, **network-based**, or **distributed/hybrid**
- Can use **anomaly detection** to identify behavior that is not that of legitimate users, or **signature/heuristic detection** to identify known malicious behavior can **block traffic** as a firewall does, but makes use of the types of algorithms developed for IDSs to determine when to do so

Host-Based IPS (HIPS)

- Can make use of either signature/heuristic or anomaly detection techniques to identify attacks
  - **Signature**: focus is on the specific content of application network traffic, or of sequences of system calls, looking for patterns that have been identified as malicious
  - **Anomaly**: IPS is looking for behavior patterns that indicate malware
- Examples of the **types of malicious behavior** addressed by a HIPS include:
  - Modification of system resources
  - Privilege-escalation exploits
  - Buffer-overflow exploits
  - Access to e-mail contact list
  - Directory traversal

HIPS

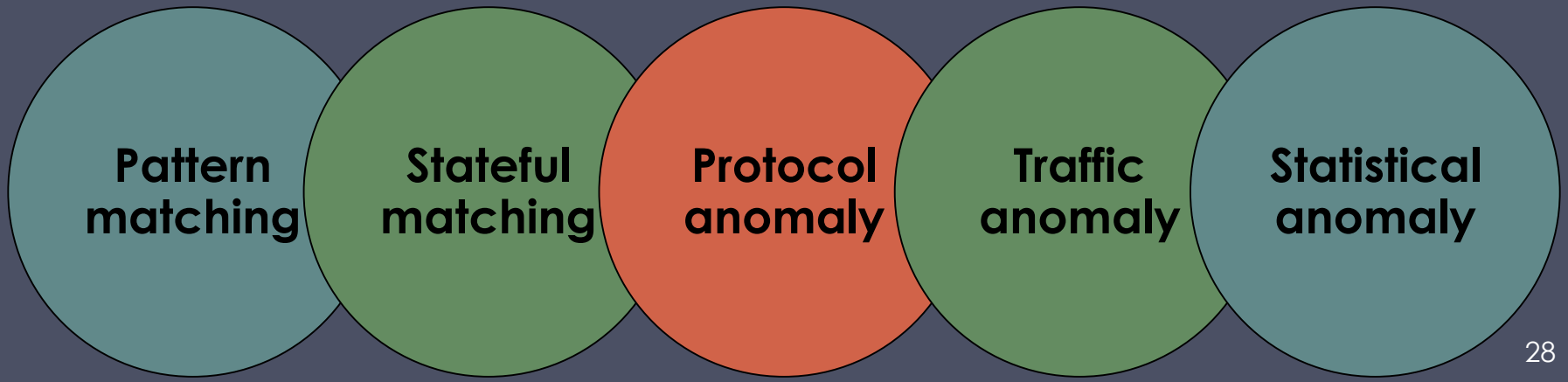
- **Capability** can be tailored to the specific platform
- A set of **general purpose tools** may be used for a desktop or server system
- Some **packages** are designed to protect specific types of servers, such as Web servers and database servers
  - In this case the HIPS looks for particular application attacks
- Can use a **sandbox approach**
  - Sandboxes are especially suited to **mobile code** such as Java applets and scripting languages
  - HIPS quarantines such code in an isolated system area then runs the code and monitors its behavior
- Areas for which a HIPS typically offers **desktop protection**:
  - System calls
  - File system access
  - System registry settings
  - Host input/output

The Role of HIPS

- Many industry observers see the **enterprise endpoint**, including desktop and laptop systems, as now the main target for hackers and criminals
  - Thus security vendors are focusing more on developing **endpoint security products**
  - Traditionally, endpoint security has been provided by **a collection of distinct products**, such as antivirus, antispyware, antispam, and personal firewalls
- Approach is an effort to provide an **integrated**, **single-product** suite of functions
  - Advantages of the **integrated HIPS approach** are that the various tools work closely together, threat prevention is more comprehensive, and management is easier
- A prudent approach is to use **HIPS** as one element in a **defense-in-depth strategy** that involves network-level devices, such as either **firewalls** or **network-based IPSs**

Network-Based IPS (NIPS)

- Inline NIDS with the **authority** to modify or discard packets and tear down TCP connections
- Makes use of **signature/heuristic detection** and **anomaly detection**
- May provide **flow data protection**
  - Requires that the application payload in a sequence of packets be reassembled
- Methods used to **identify malicious packets:**



Summary

- The need for firewalls
- Firewall characteristics and access policy
- Types of firewalls
  - Packet filtering firewall
  - Stateful inspection firewalls
  - Application-level gateway
  - Circuit-level gateway
- Firewall basing
  - Bastion host
  - Host-based firewalls
  - Personal firewall
- Firewall location and configurations
  - DMZ networks
  - Virtual private networks
  - Distributed firewalls
  - Firewall locations and topologies
- Intrusion prevention systems
  - Host-based IPS
  - Network-based IPS
  - Distributed or hybrid IPS
  - Snort inline
- Example: Unified Threat Management Products

作业

- 英文教材（第四版）P336-339
- Questions 9.1, 9.6
- Problems 9.5, 9.6